Novel Algorithm For Encryption:Hybrid of Transposition and Substitution Method

Suman Mor[1], Anurag Dagar[2], Swati Saini[2]
[1] SES,BPSMV/CSE, Sonipat, India. Email: suman.mor507@gmail.com
[2] SES,BPSMV/CSE, Sonipat, India. Email: {angelannu30, sheetu38}@gmail.com

***Abstract*— This paper presents an algorithm which is hybrib of Transposition and Substitution method.The main advantage of this approach is ,it doesn't use any key from outside because key is present within the original message.Due to this the main problem of exchanging keys securely is solved.Both Transposition and Substitution method have their own limitations.So we use both these method so that the resultant cipher is more secure and strong.**

***IndexTerms*— transposition, substitution, cipher, key, encryption, decryption**

I. Introduction

Since last one decade,it's a big challenge to send confidential data or information from one system to another system. There is a massive growth in internet and communication technologies in last decade that makes it difficult to send data securely.When a person is sending data to another person over the internet then there are lots of chances of attacks.There is a big challenge to transmit data over internet with confidentiality and integrity.To provide confidentiality,we need to encrypt data.[4]So network security and cryptography are the emerging area where people are trying to develop various new encryption algorithms in order to provide more secure data.

Cryptography is an art and science for converting a plain text into nonreadable cipher text.[2]Cryptography is of two types:1)private key cryptography:a single key is used for encryption as well as decryption process.2)public key cryptography:two keys are used,one for encryption purpose and other for decryption.These types have advantages as well as disadvantages.These both types are key based and the key value can be of any type,any order and any size.[3]

In this paper,we are purposing an encryption method which works on a block of data.Block size can be changed for more secure cipher.Block size depends upon the key value which depends on data because key is hidden in message itself.[1]Transposition method permute the message to provide security and substitution method places some other data on the place of message.To provide more secure and strong cipher we use the hybrid of these techniques.In this paper we are designing an encryption algorithm which doesn't depends on any key and uses transposition as well as substitution method.

II. Proposed Algorithm

A. Encryption

1. First we take a message(plain text) from the user which which he want to encrypt.
2. Take the first character of message and convert it into its corresponding ASCII code(decimal form),named Ach.
   - Double that decimal code means find out 2*Ach.
   - Find out the corresponding character from ASCII table and extended ASCII table (any alphabet,digit or any symbol) and replace original character with this new character
3. Repeat step 2 for each alphabet or digit number present in the original message,except blank space.
4. Find out the new converted message using step 2 and step 3.
5. Find the value of P i.e. the character which present maximum time in the new converted message.
   - If there are two characters having same occurance then select that character which is having large ASCII code value in decimal form.
6. Calculate Q=int(P) i.e. ASCII code of P in decimal form
7. Perform R=Q % 9;
8. if(R>2 && R<9) then perform K=R
   elseif(R==1||R==2||R==3)
   then perform K=R+3;
9. Form the group of 'K' characters of step 4's output including space,alphabets,digits,or any other special symbol.
10. Reverse characters of each group.
11. Finally we get our secure cipher.

B.*Decryption*

This is the reverse of encryption process.This process is done on receiver side.

1. Find out the character of cipher text which occurs maximum time i.e. named A
   - If there are two characters having same occurance then select that character which is having large ASCII decimal value.
2. Find out A's corresponding ASCII decimal code i.e.B
3. Calculate C=B%9;
4. if(C>2 && C<9) then perform K=C
   elseif(C==1||C==2||C==3) then perform K=C+3;
5. Make the group of 'K' characters of cipher text.
6. Reverse characters of each group.

© 2013 ACEEE
DOI: 01.IJNS.4.1.2

7. Perform following steps corresponding each character of cipher text

- find out the ASCII code of each character.
- Half the ASCII decimal code's value.
- Place the particular character from the ASCII table corresponding that new half code.

8. Finally we get the original plain text.

III. Implementation

A. Encryption

1) Suppose the original message is
7812881 HJG85d 82TL8H

2) This Table 1 shown below shows the output of step 2:

Table 1:Represents the output of step 2 of Encryption Algorithm

Plain text:	ASCII code (Ach)	2*Ach	Cipher text:
7	55	110	n
8	56	112	p
1	49	98	b
2	50	100	d
8	56	112	p
8	56	112	p
1	49	98	b
H	72	144	É
J	74	148	ö
G	71	142	Ä
8	56	112	p
5	53	106	j
D	100	200	+
8	56	112	p
2	50	100	d
T	84	168	¿
L	76	152	ÿ
8	56	112	p
H	72	114	r

3) Apply step 2 to all characters of plain text except blank spaces,finally we get this table.

4) Now cipher text is:
npbdppb ÉöÄpjZ% pd¿ÿpr

5) In this converted text character "p" present max. time so value of P =”p”.

6) Calculate Q=112(ASCII code of "p")

7) R=Q%9 i.e. 112%9
So R=4

8) if(4>2 && 4<8)
(true&& true)=true
Perform K=4

9) Grouping of characters according to the value of K i.e. 4
npbd ppb ÉöÄp jZ% p d¿ÿp r

10) Now reverse each group:
dbpn bpp pÄöÉ p Z% j pÿ¿d r

11) Finally cipher text is:
dbpn bpppÄöÉp Z% jpÿ¿dr

B. Decryption:

1. Find out the character which present maximum times in the cipher text
dbpn bpppÄöÉp Z% jpÿ¿dr
character "p" present maximum time,A=”p”
2. B=112 i.e. p's corresponding ASCII code
3. Calculate C=B%9
C=112%9=4
4. if(4>2 && 4<8)
(True && true)=true
So K=4
5 Make group of 'K'characters i.e. 4 characters:
dbpn bpp pÄöÉ p Z% j pÿ¿d r
6 Reverse each group:
npbd ppb ÉöÄp jZ% p d¿ÿp r
7. After performing step 7, we get output which is shown below in Table 2 :

Table 2:Represents the output of step 7 of Decryption Algorithm

Cipher text:	ASCII code (Ach)	Ach/2(half of the code)	plain text:
N	110	55	7
P	112	56	8
B	98	49	1
D	100	50	2
P	112	56	8
P	112	56	8
B	98	49	1
É	144	72	H
Ö	148	74	J
Ä	142	71	G
P	112	56	8
J	106	53	5
+	200	100	d
P	112	56	8
D	100	50	2
¿	168	84	T
Ÿ	152	76	L
P	112	56	8
R	114	72	H

8. Finally we get our original message

III. Advantages

This new algorithm has various advantages over already existing various transposition and substitution methods.

1. It provide limiting range for generation of keys i.e 3 to 8.
2. It doesn't allow key value 0,1 or 2.
3. There are less chances of Brute force attack because probability value of attack is low.
4. It provide the encryption of alphabets,digits and special characters.
5. In this algorithm we use mod function(%9),so it gives only a limiting range.
6. Final cipher is combination of alphabets,digits,special symbols and extended special symbol,so to attempt an attack is very hard or practically difficult to achieve.
7. The main advantage is that,this algorithm is not based upon a single key.There is no need of sending key to receiver because key is present within the original text.
8. Easy to decrypt the cipher to get original text.

DOI: 01.IJNS.4.1.2

9. In this we change characters with any other characters including alphabets,digits,special symbol and extended ASCII code symbol so that if in case attacker find the code then he couldn't get any meaningful code.
10. As this algorithm is based on the original text so every time we get other key value.This provide a strong encrypted message.

V. Limitation

- This is complex method to encrypt message because of its implementation.
- Use of special symbols and extended ASCII code symbol makes it complex.

VI. Conclusion

This is a hybrid approach of transposition and substitution method.Both of these approach has their limitations.Transposition only permutes the data and substitution places some other character at original character.Both of these approaches use keys.Exchanging of key is the main problem.

In this algorithm we don't use any key from outside.Key is hidden within the message so no need of exchanging keys.And we use both the method to encrypt data results in a very strong and secure cipher.

References

[1] "Transposition method for cryptography" by Satish Bansal and Rajesh Shrivastava in „The IUP Journal of Computer Sciences, Vol. V, No. 4, 2011 .

[2] Atul Kahate (2009), Cryptography and Network Security, 2nd edition, McGraw-Hill.

[3] Stallings W (1999), Cryptography and Network Security, 2nd edition, Prentice Hall.

[4] William Stallings (2003), Cryptography and Network Security, 3rd edition, Pearson Education

DOI: 01.IJNS.4.1. 2